AO 106 (REV 4/10) Affidavit for Search Warrant — AUSA Barry Jonas, (312) 886-8027

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

In the Matter of the Search of:

The Google account smilinglucy16@gmail.com, further described in Attachment A

Case Number: 16M109

APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT

I, Jason VanThomme, a Special Agent of the Federal Bureau of Investigation, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property or premises:

See Attachment A

located in the Northern District of California, there is now concealed:

See Attachment A

FILED
FEB 29 2016
MAGISTRATE JUDGE
SHEILA M. FINNEGAN

The basis for the search under Fed. R. Crim. P. 41(c) is evidence.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, United States Code, Section 1832(a)(2), (a)(4) and (a)(5)	Theft of Trade Secrets

The application is based on these facts:

See Attached Affidavit,

Continued on the attached sheet.

Applicant's Signature

JASON VANTHOMME, Special Agent, Federal Bureau of Investigation
Printed name and title

Sworn to before me and signed in my presence.

Date: February 29, 2016

Judge's signature

City and State: Chicago, Illinois

SHEILA FINNEGAN, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

I. Search Procedure

1. The search warrant will be presented to Google personnel, who will be directed to isolate those accounts and files described in Section II below.

2. In order to minimize any disruption of computer service to innocent third parties, company employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

3. Google employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant. Google shall disclose responsive data, if any, by sending to 2111 West Roosevelt Ave., Chicago, Illinois using the US Postal Service or another courier service, notwithstanding 18 U.S.C. 2252A or similar statute or code.

4. Following the protocol set out in the Addendum to this Attachment, law enforcement personnel will thereafter review information and records received from company employees to locate the information to be seized by law enforcement personnel specified in Section III below.

II. Files and Accounts to be Copied by Google Employees

a. All electronic mail, including attachments thereto, stored and presently contained in, or on behalf of, the following electronic mail address:

smilinglucy16@gmail.com

which are stored at premises owned, maintained, controlled, or operated by Google, headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

b. All existing printouts from original storage of all the electronic mail described above in Section II(a).

c. All transactional information of all activity of the electronic mail addresses and/or individual accounts described in Section II(a), including log files, dates, times, methods of connecting, ports, dial-ups.

d. All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses and/or individual accounts described above in Section II(a), including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records.

e. All records indicating the services available to subscribers of the electronic mail addresses and/or individual accounts described above in Section II(a).

III. Information to be Seized by Law Enforcement Personnel

a. All information described above in Section II that constitutes evidence concerning violations of Title 18, United States Code, Section 1832(a)(2), (a)(4), and (a)(5) as follows: Electronic files, including computer source code, computer executable programs, email messages, electronic communications, attachments, and any other electronic files that contain information regarding:

- Company A
- Company B
- Toho Technology
- Dafar Brakes
- JS Trailer also known as Jiangsu Haipeng Special Vehicles Co. Ltd.
- Items relating to the identity of the user(s) of the subject account

b. All of the records and information described in Section II (c), (d), and (e).

ADDENDUM TO ATTACHMENT A

With respect to the search of any information and records received from the free web-based electronic mail service provider, law enforcement personnel will locate the information to be seized pursuant to Section III of Attachment A, according to the following protocol.

The search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. searching for and attempting to recover any hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein.

b. surveying various file directories and the electronic mail, including attachments thereto to determine whether they include data falling within the list of items to be seized as set forth herein.

c. opening or reading portions of electronic mail, and attachments thereto, in order to determine whether their contents fall within the items to be seized as set forth herein, and/or

d. performing key word searches through all electronic mail and attachments thereto, to determine whether occurrences of language contained in

such electronic mail, and attachments thereto, exist that are likely to appear in the information to be seized described in Section III of Attachment A.

Law enforcement personnel are not authorized to conduct additional searches on any information beyond the scope of the items to be seized by this warrant.

UNITED STATES DISTRICT COURT)
)
NORTHERN DISTRICT OF ILLINOIS)

AFFIDAVIT

I, Jason VanThomme, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation. I have been so employed since approximately July 2010.

2. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to economic espionage and theft of trade secrets. I have participated in the execution of multiple federal search warrants.

3. This affidavit is made in support of an application for a warrant to search, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), for information associated with certain accounts that are stored at the premises owned, maintained, controlled, or operated by Google, a free web-based electronic mail service provider located at 1600 Amphitheatre Parkway, Mountain View, California, 94043. The account to be searched is smilinglucy16@gmail.com (hereinafter, "**Subject Account 1**"), which is further described in the following paragraphs and in Part II of Attachment A.

4. As set forth below, there is probable cause to believe that in the account, described in Part II of Attachment A, in the possession of Google, there exists evidence of violations of Title 18, United States Code, Section 1832(a)(2), (a)(4) and (a)(5). The statements in this affidavit are based on my personal

knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence of violations of Title 18, United States Code, Section 1832(a)(2), (a)(4), and (a)(5), are located in **Subject Account 1**.

BACKGROUND INFORMATION

Google

6. Based on my training and experience, I have learned the following about Google:

a. Gmail is an email service provided by Google which is available to Internet users. Subscribers obtain an account by registering on the Internet with Google. Google requests subscribers to provide basic information, such as name, gender, zip code and other personal/biographical information;

b. Google maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records often include account access information, email transaction information, and account application information;

c. Any email that is sent to a Gmail subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the email or

the subscriber's mailbox exceeds the storage limits preset by Google. If the message is not deleted by the subscriber, the account is below the maximum storage limit, and the subscriber accesses the account periodically, that message can remain on Google's servers indefinitely;

d. When the subscriber sends an email, it is initiated by the user, transferred via the Internet to Google's servers, and then transmitted to its end destination. Gmail users have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email from the Google server, the email can remain on the system indefinitely;

e. A Gmail subscriber can store files, including emails and image files, on servers maintained and/or owned by Google.

FACTS SUPPORTING PROBABLE CAUSE TO SEARCH THE SUBJECT ACCOUNT

Summary

7. Company A, a company that invents and manufactures technologies worldwide, uses proprietary business Strategic Plans that contain business trade secret information that it creates and are not publicly available to conduct its business. Zhang Jing, also known as Lucy Zhang ("Zhang"), downloaded a large amount of electronic files that consist of Company A's Strategic Plans, referred to as "STRAPs" by Company A, onto external hard drives and sent, via electronic mail (e-mail), STRAPs and other proprietary Company A documents to third parties.

8. From 2007 to 2014, while Zhang was employed by Company A and from 2013 to 2014, while she was an employee of Company A assigned to Company B, a subsidiary company of Company A, located in the Chicago area, she transmitted via e-mail, Company A's business trade secret information, including the STRAPs to her spouse, Li Zhao, also known as Johnny Li ("Li"), who was involved in several business ventures in Asia, some of which appear to be in the same business industry as Company A.

Zhang's Employment at Company A & Company B

9. According to Company A's internet website, Company A, a Fortune 100 company, is headquartered in Morris Township, New Jersey, and it has offices located worldwide to include the Americas, China, India, Asia Pacific, Europe, and the Middle East & Africa. Company A also has subsidiary companies worldwide. Company B is a subsidiary company of Company A located in the Chicago area. Company A's internet website states that it invents and manufactures technologies worldwide in the areas of Aerospace Advancements; Automation Smart Technology and Control Solutions; Cutting-Edge Performance Materials and Technologies; and Efficient Transportation Systems, among other ventures. Company B is part of Company A's Performance Materials and Technologies business group and offers advanced processes, products, and services around the world.

10. On or about December 4, 2014, I interviewed Individual A, Company A's Chief Security Officer, and Individual B, the Vice President and General

Counsel of Company B. Individuals A and B stated that Zhang began working for Company A in 2007 at Company A's Sensing and Control Department, and later at Company A's Performance Materials and Technologies department, both located in China. In or around September 2013, Zhang relocated to the United States when she was transferred to a marketing team within Company B's modular equipment department at Company B's Illinois location. As with most employees, Zhang was issued a Company A/Company B computer.

11. On or about February 20, 2015, Individual B stated that when Company A employees logged onto their Company A computer, the login screen contained a warning visible on the bottom left corner of the screen. The warning stated "Warning: The company's policies – including its Code of Business Conduct and its Acceptable Use of Information Resources Policy - govern access to this system and other information resources. The unauthorized use of any of the company's computers, electronic devices, or electronic systems is prohibited and may result in discipline and/or legal action. The company reserves the right to monitor and audit all information resources without notice. No employees or agent of the company may waive this right. Any data stored on or transmitted through the company's information resources is not private. By logging on, you expressly consent to these terms."

Employee's Code of Business Conduct, Protecting Confidential Information and Agreement

12. On or about December 23, 2014, Individual B provided me with Company A's employee documents that are provided to employees, including the Company A's Code of Business Conduct, a CD entitled "Protecting Confidential Information," an agreement entitled "Employee Agreement Relating to Trade Secrets, Proprietary and Confidential information," and records of Zhang receiving said documents. I reviewed the documents which provided the following information:

a. Company A's Code of Business Conduct informs employees that they are entrusted with Company A's confidential information and they must protect this sensitive information at all times. This generally includes any nonpublic information that might be of use to competitors or others, which may be harmful to Company A if disclosed. Examples include business or marketing plans, supplier information, product design, manufacturing processes, existing and future merchandising information and employee information. The Code of Business Conduct also informs employees to never allow others access to Company A's confidential information.

b. Zhang's personnel records indicated that on March 17, 2008, March 13, 2009, and December 4, 2012, Zhang completed the web-based training for Company A's Code of Business Conduct as discussed above.

c. The training module entitled "Protecting Confidential Information" informed employees to apply Company A's Code of Business Conduct and to identify, protect, and label confidential information. The training module advised employees that Company A has many types of confidential information including business information that consists of Customer Lists, Strategic Plans, Operating Plan/Results, Potential Acquisitions, JVs & Divestitures, Management Plans, Business Forecasts, Corporate Policies & Procedures, among other types of information. The training module further advised employees that most of its confidential information falls under the definition of a "trade secret" because it provides some economic value to Company A and Company A takes reasonable steps to keep it a secret.

d. Company A records also state that on May 17, 2013, Zhang completed a web-based training entitled "Protecting Company A's Confidential Information."

e. The agreement entitled "Employee Agreement Relating to Trade Secrets, Proprietary and Confidential information" advised in paragraph 6 of the aforementioned agreement that employees are asked to understand and agree that they will never, directly or indirectly, during or after their employment with Company A misappropriate, use or disclose Company A's Trade Secrets, Proprietary and Confidential Information except in furthering Company A's business nor will they disclose or disseminate at any time Company A's Trade Secrets, Proprietary

and Confidential Information to anyone who is not an officer, director, employee, attorney or authorized agent of Company A without the prior written consent of Company A's Law Department. Employees are also advised that they will execute any agreement relating to the protection of Company A's Trade Secrets, Proprietary and Confidential Information or such information of any third party whose intellectual property Company A is under a legal obligation to protect if Company A requests that the employee do so. The agreement also informs employees that all documents and tangible things embodying or containing Company A's Trade Secrets, Proprietary and Confidential Information are Company A's exclusive property and the employee has access to them solely for performing the duties of employment by Company A and that the employee will return all of them and all copies, facsimiles and specimens of them and any other tangible forms of Company A's Trade Secrets, Proprietary and Confidential Information in the employees possession, custody or control to Company A before leaving the employment of Company A. The employee also acknowledged that they have the right to use or practice any skill or expertise generally associated with their employment but not special or unique to Company A, but that the employee does not have the right to use, practice or disclose Company A's Trade Secrets, Proprietary and Confidential Information for their own benefit or for the benefit of any third party.

f. The agreement discussed above further defined "Trade Secrets, Proprietary and Confidential information" as information that is not generally

known in the industry in which Company A is engaged, which may be disclosed to the employee or which the employee may learn, observe, discover or otherwise acquire during, or as a result of, their employment by Company A and which includes, without limitation, any information, whether patentable, patented or not, related to any existing or contemplated products, inventions, services, technology, ideas, concepts, designs, patterns, processes, compounds, formulae, programs, devices, tools, compilations of information, methods, techniques, and including information relating to any research, development, manufacture, purchasing, engineering, know-how, business plans, sales or market methods, methods of doing business, customer lists, customer usages or requirements, or supplier information, which is owned or licensed by Company A or held by Company A in confidence.

g. Zhang's signed forms on May 7, 2012, and August 21, 2014, which stated that she agree to comply with Company A's "Employee Agreement Relating to Trade Secrets, Proprietary and Confidential information" as detailed above.

Zhang's Resignation

13. Individual A stated that in or around mid-October 2014, Zhang submitted her resignation to Company A. Individual A stated that, after she submitted her resignation, Company A learned that Zhang told several Company A employees that she had employment plans in China with Tyco, a competitor of Company A, and told other Company A employees that she had no future

employment plans. Individual A stated that as a result of the statements Zhang made to several employees that she was leaving Company A for Tyco, the several e-mails that Zhang sent to senior executives about her employment resignation, and repeated access requested by Zhang to a sensitive Company A system, Company A became suspicious and installed a database prevention tool on her Company A laptop computer. The database prevention tool allowed Company A to monitor her computer activity. As a result of the installed tool on her computer, on October 28, 2014, Company A discovered that, on that same day, Zhang downloaded approximately 11,000 files, dated between 2007 and 2014, from her Company A computer to two external hard drives. According to Individual A, a large number of the 11,000 files contained Company A proprietary information including files for Company A's strategic five year plans, which were marked as proprietary information.

14. Individual A stated that on or about October 29, 2014, employees from Company A conducted an employee exit interview of Zhang. During the exit interview, Zhang was given Company A's non-disclosure agreement which she signed. The employees then asked Zhang if she took any intellectual property from Company A, to which Zhang advised that she did not take any intellectual property. Zhang was then asked if she had intellectual property at her residence, to which Zhang advised that she did not. The employees asked Zhang if she downloaded approximately 11,000 files to two external hard drives. Zhang admitted that she

downloaded the files to two external hard drives which she was going to take with her to China for "her own personal memory." The Company A employees asked Zhang to return the two external hard drives, her Company A computer and her Company A cellular phone, which she did. Zhang was asked to resign on October 29, 2014, and was told to work from home until her last day of employment of October 31, 2014.

Interview of Zhang

15. On or about October 29, 2014, I interviewed Zhang, a legal permanent resident of the United States and a Chinese national. Zhang provided the following information:

a. Zhang received a Bachelor of Science Degree from the University of Science and Technology Beijing in Beijing, China, and a Master of Business Administration Degree at École des Ponts Business School in Shanghai, China. In 2007, Zhang started employment at Company A's office in China, where she worked in various departments. On or about September 23, 2013, Zhang was transferred to Company B located in the Chicago area. While at Company B, Zhang was still an employee of Company A. Zhang worked for Company B up until her last day of employment on or about to October 31, 2014. While at Company B, Zhang was the Director of Strategic Marketing and she worked on projects in Modular Refinery.

b. On or about October 21, 2014, Zhang submitted her employment resignation at Company A. Zhang stated that she did not have the potential for job growth at her position at Company B and she found employment as a Product Manager at another company located in the Chicago area.

c. Zhang stated that on October 28, 2014, October 29, 2014, and on several other occasions, Zhang transferred Company A files from her Company A computer to two external hard drives. Zhang stated the amount of documents she copied could have been around 11,000 files. Zhang stated that some of the documents that she transferred contained confidential information and were marked as confidential. Zhang was going to keep the documents for her personal memory to refresh herself on her work and she had no intention of disclosing the information to other companies.

d. After interviewing agents advised Zhang that downloading a company's proprietary information to benefit another company or foreign government was a criminal act, Zhang stated that it would not be smart of her and she understood that she could not provide that information to anyone. Zhang said she was only going to use the documents for her personal memory. Zhang stated that she did not have any other copies of the files that she downloaded to the hard drives nor did she transfer the files to any other devices. Zhang stated that no one from her new employer or any business or foreign government asked her to download the Company A files for their use

Transfer of Documents

16. On or about December 4, 2014, I interviewed Individual A and Individual B. The employees provided the following information:

a. Individual A stated that Company A discovered that Zhang transferred approximately 11,000 Company A documents from her Company A computer to two external hard drives. According to Individual A, many of the documents were Strategic Plans (commonly referred to as "STRAP") considered by Company A to be proprietary, trade secrets, which contained Company A financial information, pricing lists, and customer lists.

b. Individual A further stated that Company A discovered, from its review of Zhang's Company A computer, that, in addition to the downloaded files, Zhang used her Company A e-mail account lucy.zhang2@[Company A].com to transmit sensitive Company A documents to **Subject Account 1**, which appears to be Zhang's personal email account and as well as email accounts belonging to her husband, Johnny Li, including lizhaosh@gmail.com, dafarusa@hotmail.com and dafarusa@aol.com. Several of the documents that Zhang emailed to herself and to Li were Company A's STRAPs.

c. Individual A stated that he learned from Zhang's files on her Company A computer that Li resided in Torrance, California and held multiple employment positions, including many high ranking positions in different

companies, including Toho International (Toho), Dafar Brakes, and a Chinese based company referred to as JS Trailer, among others.

d. Individuals A and B stated that if the STRAPs were provided to a competitor, they could be damaging to Company A. The STRAPs do not get circulated outside of Company A and they should not be sent out in an e-mail or to a hard drive to be transmitted outside of Company A. According to Individuals A and B, the STRAPs could have helped Li expand his business in China.

Trade Secret Information

17. On or about February 26, 2015, I interviewed Individual B and Individual C, Company A's Director of Planning and Work Processes. Individuals B and C provided the following information:

a. Individuals B and C stated that Company A and Company B use the STRAPs to develop their business plans and the STRAPs are Company A's proprietary business trade secret which they take reasonable measures to protect. The STRAPs are produced once a year and is Company A's five year plan to project its future business. The STRAPs contain proprietary knowledge on Company A's challenges, weaknesses, plans of action, priorities, vendors, customers, targeted customers, and other business information which is not public knowledge. The STRAPs also contain third party information which Company A pays third parties for and has a legal responsibility to protect.

b. Individuals B and C further stated that the STRAPs give Company A an advantage over its competitors and the information is treated as a trade secret just the same as Company A would protect its secret technology. Company A restricts access to the STRAPs to only the employees who work on the STRAPs as well as to executive management.

c. In addition to a standard log-on procedure (which requires entering user identification and a password) that all Company A employees follow to gain access to their computers/Company A's server, an employee wanting to access the STRAP must enter a secure area on Company A's server. This secondary process requires an employee to submit an access request, which then has to be granted in order for the employee to access the restricted shared site where the STRAPs are stored.

d. The STRAPs are not provided to any third-party business. Company A could suffer great economic harm if the STRAPs were to be released to competitors, clients, or anyone else in the same industry as Company A. The STRAPs could be used to establish or advance a competing business, which could cause the loss of clients to Company A as well. The information from the STRAPs could also allow customers to gain an advantage in business negotiations with Company A which would also cause economic damage to Company A.

18. According to Individual A, Zhang had access to the STRAPs as part of her responsibilities at Company A and Company B.

Computer Review

19. On or about December 23, 2014, Individual B provided me Zhang's Company A computer, and the two external hard drives which Zhang downloaded the approximately 11,000 files. I turned over the Company A computer and the two external hard drives to the Regional Computer Forensics Lab, which made a mirrored image of the Company A computer and external hard drives, which I then reviewed.

Li's Business

20. I reviewed the mirrored image of the Company A computer and the two external hard drives and discovered the following regarding Li:

a. Li's employment resumes were located on Zhang's Company A computer in sub-folders under file path "402067/Personal/Johnny/CVGou." The resumes detailed that Li's employer, Toho Technology, provided products and solutions for semi-conductors, LED, PV, and automotive industry worldwide. In the resumes, Li indicated that he has made a "5 years strategic market plan for China Organization" and developed and executed a China growth strategy. The resume stated that while employed by Toho Technology, he has worked on projects related to Aerospace, Wind Energy, and others. Li also detailed that he has developed new business for the commercial aircraft business in China and the United States, specifically establishing a relationship with the Aviation Industry Corporation of China (AVIC) and the Commercial Aircraft Corporation of China Ltd. (COMAC).

b. Company A is known to have business ventures as described in Li's resume for work he had done for Toho Technology, specifically in aerospace with AVIC the COMAC and PV. PV stands for photovoltaic which is a method to convert solar energy. Toho Technology is headquartered in Japan and has a presence throughout Asia, North America, the Middle East, and Europe.

c. On or about May 23, 2011, e-mails containing proprietary marked documents, entitled "PV Module Packaging STRAP 2010" and "PV Supply China" were sent from lucy.zhang2@[Company A].com to Li's Toho Technology account, johnny.li@tohotechnology.com. The e-mails were correspondence that Zhang had with other Company A employees. The johnny.li@tohotechnology.com was deactivated on August 2, 2013.

Zhang Gmail Account/Subject Account 1

21. Based on records obtained from Google Inc. received on or about January 26, 2015, **Subject Account 1** was subscribed to Zhang Jing, created on November 14, 2005, and had a recovery e-mail address of lizhaosh@gmail.com.

22. On April 28, 2015, I obtained warrants to conduct searches of e-mail accounts subscribed to Li, including lizhaosh@gmail.com (15 M 229), dafarusa@aol.com (15 M 230), and darfarusa@hotmail.com (15 M 231). I reviewed the e-mail accounts for the transfer of Company A's proprietary documents, including the files identified as a STRAP which Company A advised contain trade secret information, as well as other Company A propriety protected documents.

23. During my review I identified several transfers of Company A's proprietary documents including STRAPs from **Subject Account 1** to lizhaosh@gmail.com and dafarusa@hotmail.com

24. From 2007 to 2013, e-mails containing the Company A's proprietary marked documents including STRAPs, were sent from **Subject Account 1**, to include the following:

a. On or about September 17, 2007, an e-mail was sent to dafarusa@hotmail.com with an attached document entitled "China Initiative: AP S&C STRAP 2003."

b. On or about November 21, 2007, an e-mail was sent to dafarusa@hotmail.com with an attached document entitled "Sensing and Control STRAP Update Medical Growth Initiative."

c. On or about December 10, 2007, an e-mail was sent to dafarusa@hotmail.com with an attached document entitled "Sensing and Control AP STRAP."

d. On or about April 12, 2008, an e-mail was sent to dafarusa@hotmail.com with an attached document entitled "2008 S&C China STRAP." The e-mail stated "Johnny, How is going on with you today? The attached China 2008-2013 Strategic plan need your comments on the structure, methodology, content etc. All the best, Lucy." The document had no proprietary markings on the pages.

e. On or about November 20, 2009, an e-mail was sent to lizhaosh@gmail.com with an attached document entitled "Wind Power" (hereinafter "Wind Power"). "Wind Power" contained Company A's customer lists and was marked "Company A confidential." "Wind Power" also contained a diagram of a wind turbine which diagram as marked "Company A propriety." Company A considered customer lists a proprietary trade secrets that was also detailed in its STRAP.

f. On or about December 17, 2009, an e-mail was sent to lizhaosh@gmail.com with an attached document entitled "Wind Energy" which appeared to be identical to "Wind Power."

g. On or about February 7, 2010, an e-mail was sent with an attached Company A document entitled "Toho Technology Strategic Plan in China: Johnny Li, February 15, 2010." The e-mail stated "I selected some slides for Toho. let me know your comments." The preceding pages of the documents were labeled as Company A confidential or proprietary and several of the pages contained customer lists and were identical to pages found in "Wind Power." Company A considered customer lists as proprietary trade secrets.

h. On or about February 12, 2010, an e-mail was sent from lizhaosh@gmail.com to **Subject Account 1** with an attached document entitled "Toho Technology Strategic Plan in China: Johnny Li, February 15, 2010" which had many of the same pages as the document that was previously sent by **Subject**

Account 1 to include the customer lists; however, the pages were now labeled as "Toho Confidential." The e-mail, which was typed in Chinese and summarily translated by a FBI linguist, states "Only keep 12 pages and additional two or three pages, put into position for each one, opportunity analysis, strategic direction (guidance), entering market methods, etc. using the simplest diagrams and language will be okay. Other are useless, writing too much will cause annoyance."

i. Following the above e-mails regarding the attachment about the Toho strategic plan in China, on or about February 13, 2010, several e-mails were sent between lizhaosh@gmail.com and **Subject Account 1** which had attached to them updated versions of the document with some changes to the Toho strategic plan in China. One in particular was from **Subject Account 1** to lizhaosh@gmail.com which contained pages from the document mentioned in paragraph 24(h), as well as a diagram about wind turbines, also appears to be identical to the wind turbine diagram found in "Wind Power," but which did not contain Company A's name or any Company A markings. The e-mail contained what appeared to be correspondence from Li that stated "From the point of view of the financial statement, estimate revenue 2010-2015? If Toho takes 2 % of the market share? Profit margin? ABB sold 1 billions to Sinovel, how much of the value Toho can contribute?... etc."

j. On or about February 16, 2010, an e-mail from lizhaosh@gmail.com was sent to **Subject Account 1** which was a forward of an e-

mail correspondence Li had with an identified individual regarding sensor business in China. Li stated

> "It was pleasure meeting you at the trade show, attached please find the opportunities we can catch in China, and let me know what we can do together to find the solution. Or, what I can do for your company to develop your sensors business in China market? Thanks."

The individual responded to Li's email, thanking him for visiting the company booth to discuss fiber optic sensing capabilities and the possible use of the individual's company for measurement on wind turbine. The e-mail from lizhaosh@gmail.com had attached to it an image of the wind turbine diagram that was in "Wind Power."

k. On or about February 19, 2010, an e-mail was sent to lizhaosh@gmail.com with an attached Company A document entitled "2010 S&C STRAP Planning Session."

l. On or about March 12, 2010, an e-mail was sent to lizhaosh@gmail.com with an attached Company A document entitled "2010 AP STRAP Sensing and Control."

m. On or about April 8, 2010, an e-mail was sent to lizhaosh@gmail.com with an attached Company A document entitled "Sensing and Control 2009 Overview."

n. On or about October 4, 2013, an e-mail was sent to lizhaosh@gmail.com with an attached document entitled "Connected Aircraft

Background." The e-mail was forwarded from a previous e-mail that Zhang and other Company A employees received.

25. I have located Company A documents that appear to be the same or similar documents sent from the **Subject Account 1** to Li's email accounts on the mirrored image of Zhang's Company A computer or the two external hard drives that she provided to Company A.

26. On or about December 8, 2014, and on March 5, 2015, I issued to Google a preservation request for **Subject Account 1**.

27. Based on my training and experience in this investigation and in other investigations, I know that individuals often retain e-mails in their account for long periods of time. Indeed, in this investigation, as described above, relevant e-mails were recovered from Li's account that had been sent or received over eight years before warrants were executed.

28. Based on my training and experience in other investigations, I believe that a search of email provider account contents often of individuals engaged in criminal conduct yields investigative leads relating to:

a. the identities of co-conspirators, customers, and other individuals engaged in theft of trade secrets offenses;

b. the contact information of co-conspirators, customers, and other individuals engaged in theft of trade secrets offenses;

c. the timing of communications among co-conspirators, customers, and other individuals involved in theft of trade secrets offenses;

d. the methods and techniques used in theft of trade secrets offenses;

e. the ownership of the accounts; and

f. further distribution and use of Company A trade secret and proprietary information.

SEARCH PROCEDURE

29. In order to facilitate seizure by law enforcement of the records and information described in Attachment A, this affidavit and application for search warrant seek authorization, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to permit employees of Google to assist agents in the execution of this warrant. In executing this warrant, the following procedures will be implemented:

a. The search warrant will be presented to Google personnel who will be directed to the information described in Section II of Attachment A;

b. In order to minimize any disruption of computer service to innocent third parties, Google employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II of Attachment A, including an exact duplicate of all information described in Section II of Attachment A;

30. Google employees will provide the exact duplicate in electronic form of the information described in Section II of the Attachment A and all information stored in those accounts and files to the agent who serves this search warrant; and

31. Following the protocol set out in the Addendum to Attachment A, law enforcement personnel will thereafter review all information and records received from Google employees to locate the information to be seized by law enforcement personnel pursuant to Section III of Attachment A.

CONCLUSION

32. Based on the above information, I respectfully submit that there is probable cause to believe that evidence of violations of Title 18, United States Code, Section 1832(a)(2), (a)(4), and (a)(5) are located within one or more computers and/or servers found at Google, headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043. By this affidavit and application, I request that the Court issue a search warrant directed to Google allowing agents to seize the electronic evidence and other information stored on the Google servers following the search procedure described in Attachment A and the Addendum to Attachment A.

FURTHER AFFIANT SAYETH NOT.

Jason VanThomme
Special Agent
Federal Bureau of Investigation

Subscribed and sworn
before me this 29th day of February, 2016

Honorable SHEILA FINNEGAN
United States Magistrate Judge